CLAIMS

What is claimed is:

1. A method for securing communications between a first device and a second device, the method comprising:

mutually authenticating the first device and the second device;

generating an integrity check value by the first device; and

sending the integrity check value with a message from the first device to the second device.

2. The method of claim 1, wherein the generating of the integrity check value comprises:

extracting a selected number of bits from a pseudo-random data stream for use as coefficients of a matrix having M rows and N columns; and

performing operations on both contents of the message and the coefficients of the matrix to generate the integrity check value.

3. The method of claim 2, wherein prior to extracting the selected number of bits from the pseudo-random data stream, the method comprises:

inputting keying material into a cipher engine performing operations in accordance with a predetermined stream cipher; and

producing the pseudo-random data stream by the cipher engine.

4. The method of claim 3, wherein the predetermined stream cipher is Data Encryption Standard in counter mode.

5. The method of claim 2, wherein the extracting of the selected number of bits includes

assigning M bits from the selected number of bits as a first column of the matrix; and

reiteratively assigning M unique bits from a remainder of the selected number of bits for each remaining column of the matrix.

6. The method of claim 5, wherein the performing of the operations includes

performing arithmetic operations on M bits from the content of the message and corresponding coefficients of the first column of the matrix to produce a first plurality of resultant values; and

performing exclusive OR operations between each of the first plurality of resultant values to produce a bit of the integrity check value.

7. The method of claim 6, wherein the arithmetic operations are bitwise multiplication operations.

8. The method of claim of claim 6, wherein the performing of the operations further includes

performing arithmetic operations on the M bits from the content of the message with corresponding coefficients for a remaining N-1 columns of the matrix to produce a second plurality of resultant values associated with each of the remaining N-1 columns; and

performing exclusive OR operations between resultant values associated with each remaining N-1 column of the matrix to produce N-1 bits of the integrity check value.

9. The method of claim 2, wherein the extracting of the selected number of bits includes

assigning M bits from the selected number of bits as a first column of the matrix; and

reiteratively reassigning the M bits in accordance with a predetermined bit rotation for columns of the matrix excluding the first column.

10. The method of claim 9, wherein the performing of the operations includes

multiplying M bits from the content of the message with corresponding coefficients of the N columns of the matrix to produce a plurality of resultant values associated with each coefficient of the matrix; and

performing exclusive OR operations on the plurality of resultant values along the N columns of the matrix to produce N bits of the integrity check value.

11. The method of claim 10, wherein the performing of the operations further includes:

reiteratively computing the integrity check value based on successive groups of bits of the message.

12. A method comprising:

computing an integrity check value for an incoming message; and

determining whether the incoming message is valid by comparing the computed integrity check value with a recovered integrity check value accompanying the incoming message.

13. The method of claim 12, wherein prior to computing the integrity check value, the method further comprises decrypting the incoming message.

14. The method of claim 13, wherein the decrypting of the incoming message includes

producing a pseudo-random data stream;

extracting a predetermined number of bits from the pseudo-random data stream; and

exclusively OR'ing portions of the incoming message with the predetermined number of bits from the pseudo-random data stream.

15. The method of claim 12, wherein the computing of the integrity check value includes

producing a pseudo-random data stream;

extracting a selected number of bits from the pseudo-random data stream to generate a matrix having M rows and N columns where M and N are positive whole numbers;

multiplying M bit values of the message with corresponding coefficients of the N columns of the matrix to produce a plurality of resultant values; and

performing exclusive OR operations between resultant values associated with each column of the matrix to produce N bits of the integrity check value.

16. The method of claim 14, wherein the computing of the integrity check value includes

extracting a selected number of bits from the pseudo-random data stream to generate a matrix having M rows and N columns;

multiplying M bit values of a first group of bits of the message with corresponding coefficients of the N columns of the matrix to produce a plurality of resultant values associated with each of the coefficients; and

performing exclusive OR operations between resultant values associated with each of the N columns of the matrix to produce N bits of the integrity check value.

17. The method of claim 16, wherein the bits associated with the selected number of bits differ from the bits associated with the predetermined number of bits.

18. An electronic system comprising:

a first device to generate an integrity check value and transmit the integrity check value along with a message; and

a second device to determine whether the message has been altered by comparing a newly generated integrity check value with the integrity check value recovered with the message.

19. The electronic system of claim 18, wherein the first device is a processor and the second device is a memory.

20. The electronic system of claim 18, wherein the first device includes an integrity check value (ICV) generator to produce an integrity check value based on a selected group of bits from a pseudo-random data stream and contents of the message.

21. A program loaded in internal memory for execution by a processor of an electronic system, the program comprising:

code for authenticating both the first device and the second device;

code for generating an integrity check value by the first device; and code for sending the integrity check value with a message from the first device to the second device.